

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-296193
(43)Date of publication of application : 17.10.2003

(51)Int.CI. G06F 12/14
G06F 15/00

(21)Application number : 2002-099575

(71)Applicant : SEIKO INSTRUMENTS INC

(22)Date of filing : 02.04.2002

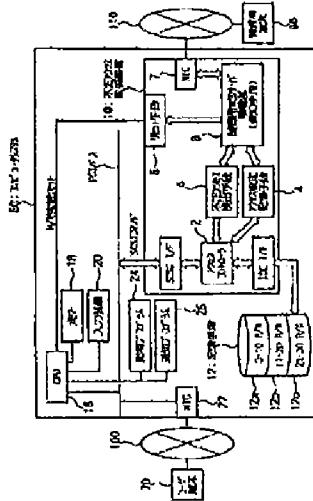
(72)Inventor : MIYAZAKI HIROSHI
SHIMIZU HIROSHI

(54) ILLICIT ACCESS MONITORING DEVICE AND METHOD, AND ILLICIT ACCESS MONITORING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an illicit access monitoring device capable of quickly detecting an illicit access to storage means of a computer system while reducing the load on the system.

SOLUTION: This illicit access monitoring device 10 is provided in a computer system 50 having storage means 12a-12c and a control means (CPU) 16. This device is provided with an access controller 2 for managing the access from the CPU to the storage means, an access set storage means 4 for storing the access set (R/W, R/O) of the storage means; an illicit access detecting means 6 for detecting an illicit access to the storage means based on the access set and the access command instructed from the CPU to the access controller; and a reporting means (controlling WEB server function part) 8 for reporting, in the detection of the illicit access, the effect to a manager terminal 80.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-296193

(P2003-296193A)

(43)公開日 平成15年10月17日(2003.10.17)

(51) Int.Cl. 12/14 320
G 06 F 15/00 310
330

F I テ-エ-ト⁺(参考)
 C 0 6 F 12/14 3 2 0 A 5 B 0 1 7
 3 1 0 H 5 B 0 8 6
 15/00 3 3 0 A

審査請求 未請求 請求項の数 6 OJ (全 6 頁)

(21) 出願番号 特願2002-99575(P2002-99575)

(71) 出願人 000002325

セイコーインスツルメンツ株式会社
千葉県千葉市美浜区中瀬1丁目8番地

(22)出願日 平成14年4月2日(2002.4.2)

(72)発明者 宮崎 宏
千葉県千葉市美浜区中瀬1丁目8番地

171

清水 洋
千葉県千葉市美浜区中瀬1丁目8番地

112-113

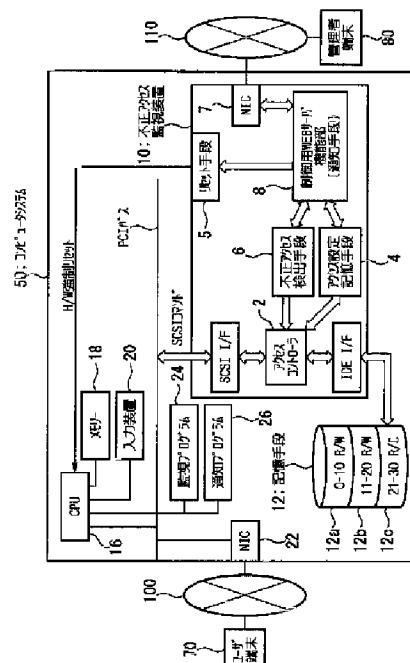
(74) 代理人 100096378
弁理士 坂上 正明
Fターム(参考) 5B017 AA08 BA01 CA07
5B085 AE00 BA06 BC02

(54) 【発明の名称】 不正アクセス監視装置及び方法、並びに不正アクセス監視プログラム

(57)【要約】

【課題】 コンピュータシステムの記憶手段への不正アクセスを迅速、かつシステムへの負荷を低減して検出できる不正アクセス監視装置を提供する。

【解決手段】 不正アクセス監視装置10は、記憶手段12a～12cと制御手段(CPU)16とを備えたコンピュータシステム50に設けられ、CPUから記憶手段へのアクセスを管理するアクセスコントローラ2と、記憶手段のアクセス設定(R/W, R/O)を記憶するアクセス設定記憶手段4と、アクセス設定とアクセスコントローラに対してCPUから指示されるアクセスコマンドとに基づき、記憶手段への不正アクセスを検出する不正アクセス検出手段6と、不正アクセスが検出されると、管理者端末80へ通知を行う通知手段(制御用WEBサーバ機能部)8とを備える。



【特許請求の範囲】

【請求項1】 記憶手段と制御手段とを備えたコンピュータシステムに設けられる不正アクセス監視装置であつて、前記制御手段から前記記憶手段へのアクセスを管理するアクセスコントローラと、前記記憶手段のアクセス設定を記憶するアクセス設定記憶手段と、前記アクセス設定と前記アクセスコントローラに対して前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する不正アクセス検出手段と、不正アクセスが検出されると、所定の通知先へ通知を行う通知手段とを備えたことを特徴とする不正アクセス監視装置。

【請求項2】 前記不正アクセス監視装置は、所定のネットワークを介して管理端末に接続され、前記通知手段は、前記管理端末に通知を行うことを特徴とする請求項1に記載の不正アクセス監視装置。

【請求項3】 前記通知手段は、前記制御手段に通知を行うことを特徴とする請求項1に記載の不正アクセス監視装置。

【請求項4】 前記通知手段からの通知、又は前記管理端末からの通知を受信して前記制御手段をリセットさせるリセット手段をさらに備えたことを特徴とする請求項1ないし3のいずれかに記載の不正アクセス監視装置。

【請求項5】 記憶手段と、バックアップ用記憶手段と、これらを制御する制御手段とを備えたコンピュータシステムで用いられ、前記制御手段から前記記憶手段へのアクセスを管理する過程と、前記記憶手段のアクセス設定を記憶する過程と、前記アクセス設定と、前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する過程と、不正アクセスが検出されると、所定の通知先へ通知を行う過程とを有することを特徴とする不正アクセス監視方法。

【請求項6】 記憶手段と、バックアップ用記憶手段と、これらを制御する制御手段とを備えたコンピュータシステムで実行される不正アクセス監視プログラムであつて、前記制御手段から前記記憶手段へのアクセスを管理する過程と、前記記憶手段のアクセス設定を記憶する過程と、前記アクセス設定と、前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する過程と、不正アクセスが検出されると、所定の通知先へ通知を行う過程とをコンピュータに実行させることを特徴とする

不正アクセス監視プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータシステム内のデータへの不正アクセスを監視するための不正アクセス監視装置及び方法、並びに不正アクセス監視プログラムに関する。

【0002】

【従来の技術】従来、コンピュータシステム（サーバシステム）への不正アクセスを監視、検出する方法として、以下が知られている。

【0003】第1の方法は、ネットワーク上を流れるパケットデータを常時監視し、不正なデータパターンや、禁止されたアクセス先が含まれているかを検出する方法である。第2の方法は、サーバのオペレーションシステム（OS）やアプリケーションが outputするログファイルを定期的に監視し、不正アクセスの結果がログファイルに残っているか否かを検出する方法である。第3の方法は、サーバのファイル内容を定期的に監視し、前回監視時と内容が異なっているか否かを検出する方法である。これらの方法は、いずれもソフトウェアを用いて検出が行われる。

【0004】

【発明が解決しようとする課題】しかしながら、上記した従来の不正アクセス監視方法の場合、ソフトウェア上で監視処理を行うのでスループットが低く、検出のタイミングが遅いという問題がある。また、サーバシステム内で監視を行う場合、システム自体がハッキングされると監視ができなくなるという問題がある。

【0005】本発明は、上記した問題点に鑑みてなされたもので、コンピュータシステムの記憶手段への不正アクセスを迅速、かつシステムへの負荷を低減して検出できる不正アクセス監視装置及び方法、並びに不正アクセス監視プログラムを提供することを目的とする。

【0006】

【課題を解決するための手段】上記した目的を達成するために、本発明の不正アクセス監視装置は、記憶手段と制御手段とを備えたコンピュータシステムに設けられ、前記制御手段から前記記憶手段へのアクセスを管理するアクセスコントローラと、前記記憶手段のアクセス設定を記憶するアクセス設定記憶手段と、前記アクセス設定と前記アクセスコントローラに対して前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する不正アクセス検出手段と、不正アクセスが検出されると、所定の通知先へ通知を行う通知手段とを備えたことを特徴とする。このような構成によれば、制御手段から記憶手段へアクセスしようとする際のアクセスコマンドを取得してアクセス設定と比較するだけでよいので、不正アクセスがあったか否かを迅速、かつシステムへの負荷を低減して検出できる。ま

た、不正アクセスが検出されると所定の通知先へ通知が可能となる。

【0007】前記不正アクセス監視装置は、所定のネットワークを介して管理端末に接続され、前記通知手段は、前記管理端末に通知を行うようにしてもよい。このようにすると、例えばコンピュータシステムの制御手段が悪意の者によってハッキングされた場合でも、制御手段の制御を受けない不正アクセス監視装置から外部の管理端末に不正アクセスを通知できる。

【0008】前記通知手段は、前記制御手段に通知を行うようにしてもよい。このようにすると、コンピュータシステム内で各種の対処を行うことができる。

【0009】前記通知手段からの通知、又は前記管理端末からの通知を受信して前記制御手段をリセットさせるリセット手段をさらに備えてもよい。このようにすると、例えばコンピュータシステムの制御手段が悪意の者によってハッキングされた場合でも、制御手段を強制的に終了させることができ、システムの安全が図られる。

【0010】本発明の不正アクセス監視方法は、前記コンピュータシステムで用いられ、前記制御手段から前記記憶手段へのアクセスを管理する過程と、前記記憶手段のアクセス設定を記憶する過程と、前記アクセス設定と、前記制御手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する過程と、不正アクセスが検出されると、所定の通知先へ通知を行う過程とを有することを特徴とする。

【0011】本発明の不正アクセス監視プログラムは、前記コンピュータシステムで実行され、前記制御手段から前記記憶手段へのアクセスを管理する過程と、前記記憶手段のアクセス設定を記憶する過程と、前記アクセス設定と、前記記憶手段から指示されるアクセスコマンドとに基づき、前記記憶手段への不正アクセスを検出する過程と、不正アクセスが検出されると、所定の通知先へ通知を行う過程とをコンピュータに実行させることを特徴とする。

【0012】

【発明の実施の形態】以下、本発明の実施の形態について、各図を参照して説明する。図1は、本発明にかかる不正アクセス監視装置10を含む不正アクセス監視システム全体の一実施の形態を示す構成ブロック図である。この不正アクセス監視システムは、Webサーバ等からなるコンピュータシステム50と、本発明の不正アクセス監視装置10とから構成される。不正アクセス監視装置10は、例えばPCI(Peripheral Component Interconnect)ボード等からなり、コンピュータシステム50のPCIスロットに挿入され、PCIバスに接続されて動作するようになっている。

【0013】コンピュータシステム50は、インターネット等の外部ネットワーク100を介してユーザ端末70に接続され、ユーザはユーザ端末70からコンピュータ

システム50内の各種データ(コンテンツ)を閲覧したり、データの更新を行えるようになっている。又、不正アクセス監視装置10は、インターネット等の内部ネットワーク110を介して管理者端末80に接続され、管理者は管理者端末80から不正アクセス監視装置10とやりとりを行う。各ネットワークとしては、専用回線、LAN(Local Area Network)、WAN(Wide Area Network)等を用いてもよい。

【0014】コンピュータシステム50は、各種データを記憶する記憶手段12(12a～12c)、CPU(制御手段)16、所定のメモリ18、キーボード等の入力装置20、外部ネットワーク100に接続される通信インターフェース(NIC)22を備えている。また、CPU16によって動作する監視プログラム24、通知プログラム26を備えている。

【0015】ここで、この実施形態では、ハードディスク等の記憶媒体からなる記憶手段12が複数のパーティション12a～12cに分割され、それぞれデータが記憶されている。各パーティションはそれぞれアクセス設定がされている。アクセス設定とは、記憶手段へのアクセス方法の設定をいい、例えば記憶手段の読み出しのみを許可して書き込みを禁止するR/O(Read Only)、記憶手段の読み出しも書き込みも許可するR/W(Read Write)がある。この実施形態では、記憶手段12のうち、セクタアドレス0～10に相当するパーティション12aがR/Wに、セクタアドレス11～20に相当するパーティション12bがR/Wに、セクタアドレス21～30に相当するパーティション12cがR/Oに、それぞれ設定されている。

【0016】記憶手段12は、不正アクセス監視装置10を介してCPU16と接続され、不正アクセス監視装置10からアクセス制御されるようになっている。なお、上記実施形態では、1つの記憶媒体(例えばハードディスク)内の領域をパーティション分割したが、別個の記憶媒体からなる複数の記憶手段としてもよい。

【0017】本発明の不正アクセス監視装置10は、アクセスコントローラ2、アクセス設定記憶手段4、リセット手段5、不正アクセス検出手段6、通知手段(制御用WEBサーバ機能部)8、内部ネットワーク110に接続される通信インターフェース(NIC:Network Interface Controller)7、図示しないメモリ等を備えている。アクセスコントローラ2、アクセス設定記憶手段4、リセット手段5、不正アクセス検出手段6、通知手段8、通信インターフェース7は、例えばプリント基板上に搭載されるCPU等から構成される。

【0018】アクセスコントローラ2は、CPU16とPCIバスを介して接続されるとともに、記憶手段12と接続され、CPU16から記憶手段12へのアクセスを管理する。なお、CPU16との接続は例えばSCSI(Small Computer System Interface)インターフェー

スが用いられ、記憶手段12との接続は例えばIDE(Integrated Device Electronics)インターフェースが用いられる。

【0019】アクセス設定記憶手段4は、記憶手段12のアクセス設定を記憶する。この実施形態では、各パーティション12a～12c毎のアクセス方法の設定、つまり、パーティション12aに該当するセクタアドレスがR/Wに、パーティション12bのセクタアドレスがR/Wに、パーティション12cのセクタアドレスがR/Oに、それぞれ設定されていることが記憶されている。アクセス設定記憶手段4へのデータの登録は、管理者端末80からNIC7、通知手段8を介して行われ、CPU16からの指示によっては登録や更新ができないようになっている。なお、アクセス設定記憶手段4をディップスイッチ等で構成し、アクセス設定を管理者が手動で行うようにしてもよく、その他のハードウェアスイッチで構成しても勿論よい。

【0020】不正アクセス検出手段6は、上記アクセス設定と、アクセスコントローラ2に対してCPU16から指示されるアクセスコマンドとに基づき、記憶手段12への不正アクセスを検出する。アクセスコマンドは次のようなものである。まず、ユーザ端末70又は入力装置20から記憶手段12への読み出し(書き込み)要求をCPU16が受信する。CPU16はこの要求をSCSI形式の読み出し(書き込み)コマンドに変換してアクセスコントローラ2に送信し、不正アクセス検出手段6はアクセスコントローラ2からこのコマンドを取得する。

【0021】通知手段(制御用WEBサーバ機能部)8は、不正アクセス検出手段6から不正アクセス検出を受信すると、所定の通知先へ通知を行う。この実施形態では、通知手段8はNIC7に接続され、内部ネットワーク110を介して管理者端末80へ不正アクセスがあった旨を通知したり、リセット手段5を介してCPU16へ信号を通知する。なお、リセット手段5はCPU16をハードウェア上で強制終了させるリセット信号を生成し、CPU16はリセット信号を通知されるようになっている。

【0022】通知手段8は、また、例えばHTML等で記述されたWebページを格納しており、管理者端末80にこのWebページを各種の設定画面として表示させる制御用WEBサーバ機能を有している。これにより、管理者は、記憶手段12のアクセス設定を画面上で行い、その設定情報は通知手段8の制御によりアクセス設定記憶手段4に登録される。また、管理者端末80からは、その他の例えば記憶手段12のパーティション設定等を行うこともできる。

【0023】なお、通知手段8を介さずにCPU16へ不正アクセスがあった旨を通知することもできる。この場合、不正アクセス検出手段6からアクセスコントローラ2へ不正アクセス検出が送信されると、アクセスコ

ントローラ2は所定のSCSIコマンドを生成してCPU16へ送信する。CPU16はこのコマンドを受信すると、監視プログラム24、通知プログラム26を順次起動し、後述する処理を行う。

【0024】次に、図2を参照して、(コンピュータシステム50の)CPU16、不正アクセス監視装置10、管理者端末80間で行われる処理フローを説明する。

【0025】この図において、まず、管理者端末80から不正アクセス監視装置10へ接続し、設定画面上で記憶手段12の書き込み禁止の設定(アクセス設定)を行う(ステップS1)。この場合、設定がされない状態では書き込み可能(R/W)とし、書き込み禁止を設定するとR/O状態になるようにしてよい。通知手段8は、アクセス設定記憶手段4にこの設定を記憶させる(ステップS3)。

【0026】次に、CPU16から記憶手段12の書き込みコマンド(SCSI)が送信されると(ステップS10)、アクセスコントローラ2はそのコマンドを不正アクセス検出手段6へ送信する(ステップS12)。不正アクセス検出手段6は、コマンドを受信すると、アクセス設定記憶手段4に記憶された設定を読み取り(ステップS14)、不正アクセスの判定を行う(ステップS16)。

【0027】判定は、例えば以下のようにして行われる。まず、不正アクセス検出手段6は、コマンドに含まれる書き込み対象領域を解析する。この領域は、記憶手段がパーティション分割されている場合、対象となるパーティションのセクタアドレスである。次に、不正アクセス検出手段6は、解析した書き込み対象領域とアクセス設定記憶手段4の設定とを比較し、その書き込み対象領域(セクタアドレス等)が書き込み禁止(R/O)に設定されている場合は不正書き込み(不正アクセス)検出と判定する。なお、この実施形態では、不正アクセス検出の有無に関わらず、書き込み禁止領域への書き込み処理自体は実行される。

【0028】以上のように、CPU16から記憶手段12へアクセスしようとする際には、アクセスコマンドが必然的にアクセスコントローラ2に送信される。従って、不正アクセス検出手段6は、アクセスコマンドを取得してアクセス設定と比較するだけでよく、不正アクセスがあったか否かを迅速、かつシステムへの負荷を低減して検出できる。特に、ハードウェア上でアクセスコマンドとアクセス設定の比較を行えば、より迅速かつ軽負荷で処理が行える。

【0029】このようにして不正書き込みが検出されると、不正アクセス検出手段6は、不正検出を通知手段8やアクセスコントローラ2へ通知する(ステップS18、S20)。通知手段8は、ステップS18で通知を受信すると、管理者端末80へ不正書き込み検出を通知す

る（ステップS22）。これにより、管理者は不正書き込みがあったことを知る。

【0030】一方、アクセスコントローラ2は、ステップS20で通知を受信すると、所定のSCSIコマンドを生成してCPU16へ送信する（ステップS24）。このSCSIコマンドは、ステップS10で受信した書き込みコマンドの情報を附加している。

【0031】CPU16は、コマンドを受信すると、監視プログラム24、通知プログラム26を順次起動する（ステップS26、S28）。監視プログラム24は、SCSIコマンドに附加された情報を参照して、書き込みを行ったプロセスID、ユーザID等を特定し、書き込み元が正規の者であるか否かを判定する。この判定は、例えば正規のシステム管理者の場合、書き込み禁止領域にも所定の情報を書き込むことがあるのを想定している。そして、正規のシステム管理者でない者による不正な書き込みであると判定すると、監視プログラム24は通知プログラム26に対して通知を指示し、通知プログラム26は所定の通知先（管理者端末80等）へ不正書き込みを通知する（ステップS30）。

【0032】本発明は上記した実施形態に限られない。例えば上記実施形態ではステップS16で、書き込み禁止領域に対して書き込みコマンドが発行されると不正アクセスと判定したが、書き込み可能領域に対して書き込みコマンドが発行された場合でも不正アクセスと判定してもよい。

【0033】前記図1の場合を例とすると、記憶手段12の各パーティションの読み書き状態（R/W、R/O）をアクセス設定とする代わりに、各パーティションに対応するセクタアドレスをアクセス設定とする。つまり、パーティション12aに相当するセクタアドレス0～10は、R/WかR/Oに関わらず書き込み禁止領域であるとみなす。従って、セクタアドレス0～10への書き込みコマンドがあると不正アクセスと判定し、管理者端末80やCPU16へ通知する。CPU16は、前述のように監視プログラムを起動し、不正アクセスと判定した者が正規のシステム管理者か否かをさらに判定する。このようにすると、セクタアドレス0～10に管理用のデータを記憶させた場合に有効である。つまり、セクタアドレス0～10には通常のユーザはアクセスしないが、管理者によるデータ更新のために書き込み可能としておく必要がある。そして、書き込みが行われた場合は仮に不正アクセスと判定し、その書き込みが正規の管理者によると判明すれば不正アクセスでなかったものとし、不正者による場合はただちに対処することができる。

【0034】なお、本発明の不正アクセス監視装置は、コンピューターと、通信装置等の各種周辺機器と、そのコンピューターによって実行されるソフトウェアプログラムとによって実現することができ、上記システム内で

実行されるソフトウェアプログラムは、コンピューター読み取り可能な記憶媒体あるいは通信回線を介して配布することが可能である。また、本発明の不正アクセス監視装置は、サーバシステムの他、パーソナルコンピュータ、ルータ、ファイアウォール等に設けることができる。

【0035】

【発明の効果】以上説明したように、本発明によれば、制御手段から記憶手段へアクセスしようとする際のアクセスコマンドを取得してアクセス設定と比較するだけでよいので、不正アクセスがあったか否かを迅速、かつシステムへの負荷を低減して検出できる。また、不正アクセスが検出されると所定の通知先へ通知が可能となる。

【0036】本発明において、不正アクセス監視装置が所定のネットワークを介して管理端末に接続され、通知手段が管理端末に通知を行うようにすると、例えばコンピュータシステムの制御手段が悪意の者によってハッキングされた場合でも、制御手段の制御を受けない不正アクセス監視装置から外部の管理端末に不正アクセスを通知できる。

【0037】本発明において、通知手段が制御手段に通知を行うようにすると、コンピュータシステム内で各種の対処を行うことができる。例えば、不正アクセスと判定した者が正規の管理者であるか否かの2次的な判定を行うことができる。

【0038】本発明において、通知手段からの通知、又は管理端末からの通知を受信して制御手段をリセットさせるリセット手段をさらに備えると、例えばコンピュータシステムの制御手段が悪意の者によってハッキングされた場合でも、制御手段を強制的に終了させることができ、システムの安全が図られる。

【図面の簡単な説明】

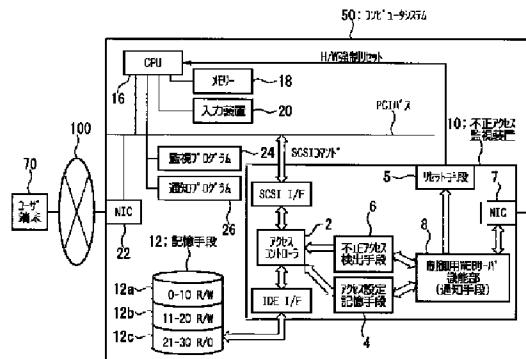
【図1】 本発明の不正アクセス監視装置を含む不正アクセス監視システム全体の構成を示すブロック図である。

【図2】 CPU、不正アクセス監視装置、管理者端末間で行われる処理のフローを示す図である。

【符号の説明】

2	アクセスコントローラ
4	アクセス設定記憶手段
6	不正アクセス検出手段
8	通知手段（制御用WEBサーバ機能部）
10	不正アクセス監視装置
12a～12c	記憶手段
16	制御手段（CPU）
50	コンピュータシステム
80	管理者端末

【図1】



【図2】

